Juegos y Rarezas Matemáticas

La Cédula de Identidad y los sorteos en Facebook

The Identity Document and the raffles on Facebook

Duberly González Molinari

Revista de Investigación

Volumen VIII, Número 2, pp. 163–176, ISSN 2174-0410
Recepción: 5 Mar'05; Aceptación: 27 Jul'18

1 de octubre de 2018

Resumen

En Uruguay, es común observar la participación de personas en sorteos de servicios o productos a través de redes sociales como Facebook, indicando para ello únicamente los últimos cuatro dígitos del número de documento de identidad. ¿Queda una persona identificada inequívocamente de esta manera? Si no es así, ¿cuántas personas comparten una terminación de estas características en su número de documento de identidad?

Palabras Clave: Cédula de Identidad, Sorteo, Facebook, Red Social, Dígito verificador.

Abstract

In Uruguay, it is common to observe the participation of people in raffles of services or products through social networks such as Facebook, indicating only the last four digits of the identity document number. Is there a person identified unequivocally in this way? If not, how many people have a termination of these characteristics in their identity document number?

Keywords: Identity Document, Raffle, Facebook, Social Network, Control number.

1. Motivación y objetivos

Es común ver en la red social *Facebook* la realización de sorteos por parte de empresas u organizaciones con el cometido de promocionar sus productos o servicios. Lo mismo sucede en ciertos programas radiales donde se escucha hablar de sorteos de entradas al cine, etc.

En los casos mencionados y en otros que se nos pueda ocurrir, la forma de participar es sencilla: el participante da *Me gusta* a la página de quien organiza el sorteo y/o a la publicación en cuestión, además de compartirla en forma pública, obviamente, con el objetivo por parte de dicha organización de ganar en publicidad.

Sin embargo, en muchos de dichos sorteos, además, se pide que el participante indique los cuatro últimos dígitos del número de su Cédula de Identidad (C.I.). Ejemplo: Mi número de C.I.

es 4.378.273-8, con lo que, para participar de alguno de dichos sorteos, yo debería indicar: 273-8.

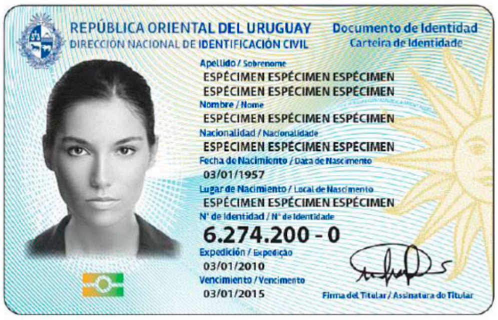

Figura 1. Modelo de C.I. uruguaya

La pregunta que surge es la siguiente: Si la intención de quien o quienes organizan dichos sorteos es requerir la anterior información con objeto de identificar inequívocamente al participante, ¿queda una persona totalmente identificada conociendo únicamente los cuatro últimos dígitos de su número de C.I.?

Haciendo un simple razonamiento, la respuesta es claramente: ¡No! ¿Por qué? Pues, podrían existir un total de 10.000 posibles terminaciones para un número de C.I.: del 000-0 al 999-9. En caso de que participasen de uno de los mencionados sorteos, un número de personas superior a 10.000, habrían al menos 2 personas ganadoras y recordemos que por lo general, estos sorteos, premian a un sólo ganador, o distinguen entre primer premio, segundo premio, etc.

Es obvio que quienes organizan estos sorteos entienden ciertas características como evidentes:

1. La cantidad de participantes no es en general un número muy elevado.

2. La persona que participa, ya sea publicando en Facebook o enviando un mensaje por Whatsapp, de alguna manera, está indicando su nombre o apodo como para que la identificación se haga sin problemas (o con menos problemas).

En definitiva, este trabajo intentará mostrar que para cualquier terminación de un número de C.I. como se dijo anteriormente, existirá un número fijo de posibles Cédulas de Identidad con igual terminación, independientemente de cual sea dicha terminación.

En tal sentido, comenzaremos describiendo el procedimiento para determinar lo que se conoce con el nombre de *dígito verificador*, es decir, el dígito que aparece luego del guión en la escritura de cualquier número de C.I.

Para comprender el tratamiento que se hará en las próximas líneas, basta con manejar conceptos básicos de divisibilidad en $\mathbb{N}$ y se aprovechará para introducir (en caso que el lector no lo maneje) conceptos básicos de la *aritmética modular*, por lo que el presente trabajo, podría servir como un breve material didáctico a utilizar en forma complementaria en cursos tales como el de Matemática II de 5to Científico del Plan Ref. 2006 de Educación Secundaria de la República Oriental del Uruguay [1].

[1] El curso de Matemática II de 5to Científico del Plan Ref. 2006 de Educación Secundaria de Uruguay está destinado a jóvenes que rondan los 17 años de edad e incluye temas como inducción y divisibilidad en $\mathbb{N}$, entre otros.

2. Dígito verificador de la C.I.

El *dígito verificador* de la C.I. es el dígito que aparece en último lugar (luego del guión) en cualquier número de C.I. Su nombre se debe al hecho de que el mismo se calcula a partir de los siete números anteriores (o seis en algunos pocos casos). Veamos un ejemplo:

Mi número de C.I. comienza así:

$$4.378.273 - X$$

Obtengamos el *dígito verificador* X:

1. Comenzamos multiplicando cada uno de los dígitos del número de C.I. en forma respectiva por los dígitos del número 2987634, es decir:

$$\begin{aligned} 4 \times 2 &= 8 \\ 3 \times 9 &= 27 \\ 7 \times 8 &= 56 \\ 8 \times 7 &= 56 \\ 2 \times 6 &= 12 \\ 7 \times 3 &= 21 \\ 3 \times 4 &= 12 \end{aligned}$$

   La elección del *número de control* 2987634 no es arbitraria. El mismo permite detectar y corregir errores en la transmisión de la información, por ejemplo, cuando ingresamos nuestro número de C.I. en un formulario electrónico e intercambiamos, de forma errónea, dos dígitos de lugar.

2. En segundo lugar, de los resultados obtenidos, consideraremos únicamente los dígitos de las unidades. Observemos que, en el sistema decimal, se puede obtener el dígito de las unidades de un número natural n, hallando el resto r de la división entera de n entre 10, es decir:

$$\begin{array}{r|l} 8 & 10 \\ \hline 8 & 0 \end{array} \Rightarrow r = 8$$

$$\begin{array}{r|l} 27 & 10 \\ \hline 7 & 2 \end{array} \Rightarrow r = 7$$

$$\begin{array}{r|l} 56 & 10 \\ \hline 6 & 5 \end{array} \Rightarrow r = 6$$

$$\begin{array}{r|l} 12 & 10 \\ \hline 2 & 1 \end{array} \Rightarrow r = 2$$

$$\begin{array}{r|l} 21 & 10 \\ \hline 1 & 2 \end{array} \Rightarrow r = 1$$

3. En tercer lugar, sumamos los resultados obtenidos en el ítem anterior:

$$8 + 7 + 6 + 6 + 2 + 1 + 2 = 32$$

4. En cuarto lugar, nuevamente consideramos el dígito de las unidades del número que acabamos de obtener, o sea:

$$\begin{array}{r|l} 32 & 10 \\ \hline 2 & 3 \end{array} \Rightarrow r = 2$$

5. En penúltimo lugar, calculamos la diferencia entre 10 y el número hallado recientemente:

$$10 - 2 = 8$$

6. Por último, obtenemos el resto entero que resulta de dividir el número obtenido recientemente, entre 10:

$$\begin{array}{r|l} 8 & 10 \\ \hline 8 & 0 \end{array} \Rightarrow r = 8$$

El número así obtenido es el *dígito verificador* de mi número de C.I., es decir: $X = 8$.

Observemos que en los pasos 5. y 6. se obtuvieron los mismos resultados, por lo que se podría pensar que el último paso es innecesario, lo cual no es correcto, ya que si en el paso 4. el resultado obtenido hubiera sido $r = 0$, el paso 5. nos llevaría a que $10 - 0 = 10$, con lo que, en el paso 6., se llegaría a $r = 0$, y, por tanto, los números obtenidos en los ítems 5. y 6. difieren.

Enunciaremos ahora ciertas definiciones y propiedades que harán que el estudio que nos proponemos, sea más sencillo de abordar.

3. Congruencia

Definición 3.1. Dos naturales a y b se llaman *congruentes según el módulo m*, lo que se indica como: $a \equiv b \pmod{m}$ si, al dividirlos por m, se obtienen restos iguales.

Expresado simbólicamente, si denotamos con $a \bmod m$ al resto de dividir a entre m, tenemos que:

$$a \equiv b \pmod{m} \;\Leftrightarrow\; a \bmod m = b \bmod m$$

Teorema 3.1. La condición necesaria y suficiente para que $a \equiv b \pmod{m}$ es que, siendo $a \geq b$, sea $a - b = \dot{m}$. (Si fuese $b \geq a$ la condición sería $b - a = \dot{m}$.)

Demostración: ($\Longrightarrow$) Por hipótesis: $a = hm + r$ y $b = km + r$, con $h \geq k$.

Entonces: $a - b = hm + r - (km + r) = (h - k)m = \dot{m}$, lo cual prueba la tesis.

($\Longleftarrow$) Por hipótesis: $a = b + \dot{m}$ y, siendo $b = km + r$, con $r < m$, es: $a = km + r + \dot{m} = \dot{m} + r$, con lo que r es también el resto de dividir a entre m.

El teorema queda así completamente probado. ■

Teorema 3.2. Sean a, b, c, d y m, naturales con $m \neq 0$. Si $a \equiv b \pmod{m}$ y $c \equiv d \pmod{m}$, entonces $a + c \equiv b + d \pmod{m}$

Demostración: Por hipótesis: $a = b + \dot{m}$ y $c = d + \dot{m}$.

Si sumamos miembro a miembro esas igualdades, obtenemos:

$a + c = b + d + \dot{m} + \dot{m} = b + d + \dot{m}$, lo cual, de acuerdo con el teorema anterior, es equivalente a la tesis. ■

Teorema 3.3. Si $a_i \equiv b_i \pmod{m}$ para $1 \leq i \leq n$, entonces

$$\sum_{i=1}^{n} a_i \equiv \sum_{i=1}^{n} b_i \pmod{m}$$

DEMOSTRACIÓN: Para $n = 1$, la demostración es trivial. Procederemos, para el resto de los casos, por inducción completa.

Base inductiva. Veamos que es cierto para $n = 2$. En efecto, por el teorema anterior,

$$\left.\begin{array}{l} a_1 \equiv b_1 \pmod{m} \\ \\ a_2 \equiv b_2 \pmod{m} \end{array}\right\} \Longrightarrow a_1 + a_2 \equiv b_1 + b_2 \pmod{m} \Longrightarrow$$

$$\sum_{i=1}^{2} a_i \equiv \sum_{i=1}^{2} b_i \pmod{m}$$

Hipótesis inductiva. Supongamos que la proposición es cierta para $n = h$, es decir, si $a_i \equiv b_i \pmod{m}$, $i = 1, 2, \ldots, h$, entonces

$$\sum_{i=1}^{h} a_i \equiv \sum_{i=1}^{h} b_i \pmod{m}$$

Veamos que también se cumple para $n = h + 1$. En efecto, si

$$a_i \equiv b_i \pmod{m},\ i = 1, 2, \ldots, h, h+1$$

entonces por la *Hipótesis inductiva* y por el teorema anterior, tendremos que

$$\left.\begin{array}{l} \displaystyle\sum_{i=1}^{h} a_i \equiv \sum_{i=1}^{h} b_i \pmod{m} \\ \\ a_{h+1} \equiv b_{h+1} \pmod{m} \end{array}\right\} \Longrightarrow \sum_{i=1}^{h} a_i + a_{h+1} \equiv \sum_{i=1}^{h} b_i + b_{h+1} \pmod{m} \Longrightarrow$$

$$\sum_{i=1}^{h+1} a_i \equiv \sum_{i=1}^{h+1} b_i \pmod{m}$$

y, consecuentemente, la proposición será cierta para todo n ■

Teorema 3.4. Sean a y m naturales con $m \neq 0$, entonces $a \equiv a \bmod m \pmod{m}$

DEMOSTRACIÓN: En efecto, al dividir a entre m, se tiene que $a = mq + r$, de donde $a - r = mq$, es decir, $a - a \bmod m = \dot{m}$ y aplicando el **Teorema 3.1** se tiene que: $a \equiv a \bmod m \pmod{m}$ ■

Teorema 3.5. Sean a_i y m naturales para $1 \leq i \leq n$ con $m \neq 0$, entonces

$$\left(\sum_{i=1}^{n} a_i \bmod m\right) \bmod m = \left(\sum_{i=1}^{n} a_i\right) \bmod m$$

DEMOSTRACIÓN: Aplicando el **Teorema 3.4**, se tiene que $a_i \equiv a_i \bmod m \pmod{m}$ para $1 \leq i \leq n$ y aplicando ahora el **Teorema 3.3** se tiene que

$$\sum_{i=1}^{n} a_i \equiv \sum_{i=1}^{n} a_i \bmod m \pmod{m}$$

luego, aplicando la **Definición 3.1** se tiene

$$\left(\sum_{i=1}^{n} a_i\right) \bmod m = \left(\sum_{i=1}^{n} a_i \bmod m\right) \bmod m \ ■$$

Teorema 3.6. Una condición necesaria y suficiente para que $a \operatorname{mód.} m = b \operatorname{mód.} m$ es que sea $(m - a \operatorname{mód.} m) \operatorname{mód.} m = (m - b \operatorname{mód.} m) \operatorname{mód.} m$

DEMOSTRACIÓN: En efecto, aplicando la **Definición 3.1**, el **Teorema 3.1** y operando, se tienen las siguientes equivalencias:

$$(m - a \operatorname{mód.} m) \operatorname{mód.} m = (m - b \operatorname{mód.} m) \operatorname{mód.} m \Leftrightarrow$$

$$m - a \operatorname{mód.} m \equiv m - b \operatorname{mód.} m \,(\operatorname{mód.} m) \Leftrightarrow$$

$$m - a \operatorname{mód.} m - m + b \operatorname{mód.} m = \dot{m} \Leftrightarrow$$

$$b \operatorname{mód.} m - a \operatorname{mód.} m = \dot{m} \Leftrightarrow$$

$$b \operatorname{mód.} m \equiv a \operatorname{mód.} m \,(\operatorname{mód.} m) \Leftrightarrow$$

$$(a \operatorname{mód.} m) \operatorname{mód.} m = (b \operatorname{mód.} m) \operatorname{mód.} m \quad \text{(I)}$$

Por otra parte, el **Teorema 3.4** establece que para a y m naturales con $m \neq 0$, se tiene que $a \equiv a \operatorname{mód.} m \,(\operatorname{mód.} m)$, es decir, $a \operatorname{mód.} m = (a \operatorname{mód.} m) \operatorname{mód.} m$. Aplicando este resultado en (I), se concluye la prueba. ■

Teorema 3.7. Una condición necesaria y suficiente para que $a \operatorname{mód.} m = b \operatorname{mód.} m$ es que sea $(a + c) \operatorname{mód.} m = (b + c) \operatorname{mód.} m$

DEMOSTRACIÓN: Nuevamente, aplicando la **Definición 3.1** y el **Teorema 3.1** se tiene que:

$$(a + c) \operatorname{mód.} m = (b + c) \operatorname{mód.} m \Leftrightarrow$$

$$a + c \equiv b + c \,(\operatorname{mód.} m) \Leftrightarrow$$

$$a + c - b - c = \dot{m} \Leftrightarrow$$

$$a - b = \dot{m} \Leftrightarrow$$

$$a \equiv b \,(\operatorname{mód.} m) \Leftrightarrow$$

$$a \operatorname{mód.} m = b \operatorname{mód.} m \blacksquare$$

Teorema 3.8. La ecuación $ax + by = c$ tiene solución entera si y sólo si $D|c$, donde $D = MCD(a, b)$

DEMOSTRACIÓN: ($\Longrightarrow$) Como $D = MCD(a, b)$, se tiene que $D|a$ y $D|b$ y, por tanto, $D|ax$ y $D|by$ siendo (x, y) una solución de la ecuación $ax + by = c$.

Por último, al ser $D|ax$ y $D|by$ se tiene que $D|ax + by$, es decir, $D|c$.

($\Longleftarrow$) Al hecho de ser $D|a$ y $D|b$ sumémosle el hecho de que $D|c$.

Dividiendo, por tanto, la ecuación original entre D, obtenemos la siguiente ecuación equivalente:

$$a'x + b'y = c'$$

donde $a' = \frac{a}{D}$, $b' = \frac{b}{D}$ y $c' = \frac{c}{D}$.

Por otra parte, observemos que $MCD(a', b') = 1$ por lo que aplicando la *identidad de Bézout* se tiene que existen enteros x_0' e y_0' tales que:

$$a'x_0' + b'y_0' = 1$$

y multiplicando por c' esta última igualdad se obtiene:

$$a'(c'x_0') + b'(c'y_0') = c'$$

lo que muestra que $x_0 = c'x_0'$ e $y_0 = c'y_0'$ son soluciones de la ecuación $a'x + b'y = c'$ y, por tanto, de su equivalente $ax + by = c$. ■

Teorema 3.9. Si la ecuación $ax + by = c$ tiene solución entera y (x_0, y_0) es una solución particular, entonces toda otra solución (x, y) es de la forma

$$x = x_0 + \frac{b}{D}t, \quad y = y_0 - \frac{a}{D}t$$

donde t es cualquier entero

DEMOSTRACIÓN: Primero probaremos que efectivamente x e y son soluciones de la ecuación $ax + by = c$:

$$a\left(x_0 + \frac{b}{D}t\right) + b\left(y_0 - \frac{a}{D}t\right) = ax_0 + \frac{ab}{D}t + by_0 - \frac{ab}{D}t = ax_0 + by_0 = c$$

Por otra parte, como se dijo en el teorema anterior, (x, y) es solución de la ecuación $ax + by = c$ si y sólo si lo es de:

$$a'x + b'y = c'$$

con $a' = \frac{a}{D}$, $b' = \frac{b}{D}$ y $c' = \frac{c}{D}$ y, por tanto, se cumplirá:

$$a'(x - x_0) + b'(y - y_0) = c' - c' = 0$$

de donde

$$a'(x - x_0) = -b'(y - y_0)$$

De esto se deduce que $a' | -b'(y - y_0)$ y al ser a' y b' coprimos, llegamos a que $a' | y_0 - y$. Luego, $y = y_0 - a't$, o sea, $y = y_0 - \frac{a}{D}t$ siendo t entero.

En forma similar se deduce que $x = x_0 + b's$ con s entero.

Resta probar que $s = t$ y para ello sustituimos la solución (x, y) en la ecuación $a'x + b'y = c'$:

$$a'(x_0 + b's) + b'(y_0 - a't) = c' \Rightarrow \underbrace{a'x_0 + b'y_0}_{=c'} + a'b'(s - t) = c' \Rightarrow a'b'(s - t) = 0 \Rightarrow s = t$$

Por tanto, tenemos que $x = x_0 + \frac{b}{D}t$. ■

Teorema 3.10. La ecuación $ax \equiv b \pmod{m}$ tiene solución si y sólo si $D | b$, donde $D = MCD(a, m)$. Si x_0 es una solución particular, entonces la solución general viene dada por

$$x \equiv x_0 \left(\text{mód.}\ \frac{m}{D}\right)$$

DEMOSTRACIÓN: Por el **Teorema 3.1.**, la ecuación $ax \equiv b \pmod{m}$ puede expresarse como:

$$ax - my = b$$

la cual, según los dos teoremas anteriores, tiene solución y además la solución general para x está dada por:

$$x = x_0 + \frac{m}{D}t \Leftrightarrow x \equiv x_0 \left(\text{mód.}\ \frac{m}{D}\right) \blacksquare$$

Observación: Nótese que

$$x_0,\ x_0 + \frac{m}{D},\ x_0 + \frac{2m}{D},\ \ldots, x_0 + \frac{(D-1)m}{D}$$

son D soluciones distintas según el módulo m.

Teorema 3.11. La ecuación

$$\sum_{i=1}^{n} a_i x_i \equiv c \pmod{m}$$

tiene solución si y sólo si $D|c$, donde $D = MCD(a_1, a_2, \ldots, a_n, m)$.

El número de soluciones distintas según el módulo m es Dm^{n-1}.

DEMOSTRACIÓN: Para el caso particular $n = 1$ se tiene el **Teorema 3.10.**

Para $n = 2$: ($\Longrightarrow$) Como $D = MCD(a_1, a_2, m)$, tenemos que $D|a_1$, $D|a_2$ y $D|m$, de donde $D|a_1x_1'$, $D|a_2x_2'$ y $D|\dot{m}$ y, por tanto, se puede afirmar que

$$D|a_1x_1' + a_2x_2' - \dot{m} \qquad \text{(I)}$$

siendo (x_1', x_2') una solución de la ecuación $a_1x_1 + a_2x_2 \equiv c \pmod{m}$.

Por otra parte, como $a_1x_1' + a_2x_2' \equiv c \pmod{m}$ se tiene que $a_1x_1' + a_2x_2' - c = \dot{m}$, de donde

$$a_1x_1' + a_2x_2' - \dot{m} = c \qquad \text{(II)}$$

De (I) y (II) se concluye que $D|c$.

($\Longleftarrow$) Como $a_1x_1 + a_2x_2 \equiv c \pmod{m}$, tenemos que $a_1x_1 + a_2x_2 - c = \dot{m}$ o, su equivalente

$$a_1x_1 - c = \dot{m} - a_2x_2 \quad \text{(III)}$$

Ahora, si convenimos en llamar $D' = MCD(a_2, m)$, es claro que el segundo miembro de (III) es múltiplo de D' y, por tanto:

$$a_1x_1 - c = \dot{D}' \Longleftrightarrow a_1x_1 \equiv c \pmod{D'} \quad \text{(IV)}$$

Por otra parte, observemos que $MCD(a_1, D') = MCD(a_1, MCD(a_2, m)) = MCD(a_1, a_2, m) = D$ y además $D|c$, y en virtud del **Teorema 3.10.**, la ecuación (IV) tiene D soluciones distintas módulo D', a saber:

$$x_1 = x_1' + \frac{D'}{D}t \quad \text{con} \quad t = 0, 1, \ldots, D-2, D-1$$

o su equivalente

$$x_1 = x_1' + \frac{D'm}{Dm}t \quad \text{con} \quad t = 0, 1, \ldots, \frac{Dm}{D'} - 2, \frac{Dm}{D'} - 1$$

es decir, $\frac{Dm}{D'}$ soluciones distintas módulo m para x_1.

Para cada solución de x_1, se sustituye su valor en la ecuación

$$a_1 x_1 + a_2 x_2 \equiv c \, (\text{mód.}\, m)$$

para obtener:

$$a_1 x_1 + a_2 x_2 - c = \dot{m} \Rightarrow a_2 x_2 - (c - a_1 x_1) = \dot{m} \Rightarrow a_2 x_2 \equiv c - a_1 x_1 \, (\text{mód.}\, m) \quad \text{(V)}$$

Recordando que $D' = MCD(a_2, m)$ y además $D' | c - a_1 x_1$, nuevamente, por el **Teorema 3.10.** se tiene que la ecuación (V) tiene D' soluciones distintas módulo m para x_2.

Por último, la ecuación $a_1 x_1 + a_2 x_2 \equiv c \, (\text{mód.}\, m)$ tendrá $S = S_{x_1} \times S_{x_2}$ soluciones, siendo S_{x_1} el número de soluciones para x_1 y S_{x_2} el número de soluciones para x_2, es decir:

$$S = \frac{Dm}{D'} \cdot D' = Dm$$

Para demostrar el caso general $\forall n, n \in \mathbb{N}, n > 2$ se puede usar inducción completa considerando los casos base anteriores. ■

4. Modelizando el problema

Con las herramientas desarrolladas en el capítulo anterior, estamos en condiciones de abordar el problema que nos proponemos, es decir, considerando un número de C.I. genérico

$$a\,.\,b\,c\,d\,.\,e\,f\,g - X$$

con a, b, c, d, e, f y g naturales menores que 10, probar la existencia de un número de C.I.

$$a'\,.\,b'\,c'\,d'\,.\,e\,f\,g - X$$

con a', b', c' y d' naturales menores que 10 y que cumplan, además, con al menos una de las siguientes condiciones: $a \neq a'$, $b \neq b'$, $c \neq c'$, $d \neq d'$.

Como el *dígito verificador* es función de los anteriores, comenzaremos calculando el mismo para ambos números de C.I. con el procedimiento descrito en la sección 2 e imponiendo, al final, su igualdad.

Para el número $a\,.\,b\,c\,d\,.\,e\,f\,g - X$, tendremos:

1. Multiplicamos cada uno de los dígitos del número de C.I. en forma respectiva por los dígitos del número 2987634:

$$\begin{aligned} a \times 2 &= 2a \\ b \times 9 &= 9b \\ c \times 8 &= 8c \\ d \times 7 &= 7d \\ e \times 6 &= 6e \\ f \times 3 &= 3f \\ g \times 4 &= 4g \end{aligned}$$

2. De los resultados obtenidos, consideramos únicamente los dígitos de las unidades:

$$\begin{gathered}2a \bmod 10\\ 9b \bmod 10\\ 8c \bmod 10\\ 7d \bmod 10\\ 6e \bmod 10\\ 3f \bmod 10\\ 4g \bmod 10\end{gathered}$$

3. Sumamos los resultados obtenidos:
   $2a \bmod 10 + 9b \bmod 10 + 8c \bmod 10 + 7d \bmod 10 + 6e \bmod 10 + 3f \bmod 10 + 4g \bmod 10$

4. Consideramos el dígito de las unidades del número que acabamos de obtener:
   $(2a \bmod 10 + 9b \bmod 10 + 8c \bmod 10 + 7d \bmod 10 + 6e \bmod 10 + 3f \bmod 10 + 4g \bmod 10) \bmod 10$
   Antes de seguir, observemos que por el **Teorema 3.5**, esta última expresión es equivalente a:
   $$(2a + 9b + 8c + 7d + 6e + 3f + 4g) \bmod 10$$

5. Calculamos la diferencia entre 10 y el número hallado recientemente:
   $$10 - (2a + 9b + 8c + 7d + 6e + 3f + 4g) \bmod 10$$

6. Calculamos el resto de dividir el número obtenido recientemente, entre 10, el cual será el *dígito verificador*:
   $$X = (10 - (2a + 9b + 8c + 7d + 6e + 3f + 4g) \bmod 10) \bmod 10$$

Es obvio que, para el número de C.I. $a' \,.\, b'\, c'\, d' \,.\, e\, f\, g - X$, se tendrá:

$$X = \big(10 - \big(2a' + 9b' + 8c' + 7d' + 6e + 3f + 4g\big) \bmod 10\big) \bmod 10$$

Igualando estas dos últimas expresiones, se tiene que:

$$\begin{gathered}(10 - (2a + 9b + 8c + 7d + 6e + 3f + 4g) \bmod 10) \bmod 10\\ =\\ \big(10 - \big(2a' + 9b' + 8c' + 7d' + 6e + 3f + 4g\big) \bmod 10\big) \bmod 10\end{gathered}$$

Si ahora aplicamos el **Teorema 3.6**, la expresión anterior es equivalente a:

$$\begin{gathered}(2a + 9b + 8c + 7d + 6e + 3f + 4g) \bmod 10\\ =\\ \big(2a' + 9b' + 8c' + 7d' + 6e + 3f + 4g\big) \bmod 10\end{gathered}$$

Asociando convenientemente los términos encerrados entre paréntesis y por el **Teorema 3.7**, la igualdad anterior se cumplirá si y sólo si:

$$\big(2a' + 9b' + 8c' + 7d'\big) \bmod 10 = (2a + 9b + 8c + 7d) \bmod 10$$

Esta última expresión es equivalente a:

$$2a' + 9b' + 8c' + 7d' \equiv 2a + 9b + 8c + 7d \,(\text{mód.}\, 10)$$

Por último, dado que los valores de a, b, c y d son conocidos, pero no así los valores de a', b', c' y d' y observando además que $MCD(2, 9, 8, 7, 10) = 1$ y $1|2a + 9b + 8c + 7d$, en virtud del **Teorema 3.11.** estamos en condiciones de afirmar que:

La ecuación

$$2a' + 9b' + 8c' + 7d' \equiv 2a + 9b + 8c + 7d \,(\textit{mód.}\, 10)$$

tiene $1 \cdot 10^{4-1} = 1000$ *soluciones distintas módulo* 10.

Traduciendo el enunciado anterior, podemos entonces concluir que:

Dado un número de C.I.

$$a\,.\,b\,c\,d\,.\,e\,f\,g\;-\;X$$

con a, b, c, d, e, f, g *y* X *naturales menores que* 10 *tales que*

$$X = (10 - (2a + 9b + 8c + 7d + 6e + 3f + 4g)\ \textit{mód.}\, 10)\ \textit{mód.}\, 10,$$

existen 1000 *números de C.I. (inclusive el número dado) de la forma*

$$a'\,.\,b'\,c'\,d'\,.\,e\,f\,g\;-\;X$$

con a', b', c' *y* d' *naturales menores que* 10.

5. Implementación en *Python*

El presente capítulo pretende ser breve y mostrar los resultados obtenidos en el capítulo anterior mediante la ejecución de un programa cuyo código fue escrito a tales efectos en lenguaje de programación *Python*.

El programa simplemente comienza solicitando al usuario que ingrese su número de Cédula de Identidad sin puntos, guión y dígito verificador. En dicho caso, se le muestra en pantalla al usuario el dígito verificador del número de Cédula de Identidad ingresado así como también la cantidad total de números de Cédulas de Identidad con la misma terminación (tres últimos dígitos más el dígito verificador) y dichos números.

Como era de esperar, la prueba para el número de Cédula de Identidad tomado como ejemplo: $4\,.\,378\,.\,273\;-\;8$, arroja que existen 1000 números de Cédula de Identidad (incluida esta) con la misma terminación $(273\;-\;8)$ y muestra a los mismos, todo esto en un tiempo de $0,028$ segundos aproximadamente.

El siguiente es el código de dicho programa:

```
# -*- coding: utf-8 -*-
from time import time
fin="n"
while fin not in ["s","S","si","SI","Si","sI","sí","SÍ","Sí","sÍ"]:
    print; print; print "Ingrese su número de Cédula de Identidad sin puntos ni guión ni dígito verificador. Luego presione Enter."
    print; print "Ejemplo: Si su número de Cédula de Identidad es 1.234.567-8, debe ingresar 1234567"
    print
    ci=input("Número de Cédula de Identidad: ")
    print
    def ci_a_lista(n):
        l=[]
```

```
        while n!=0:
            l=[n%10]+l
            n=n//10
        return l
    def completa_lista(n):
        l=ci_a_lista(n)
        if len(l)==7:
            return l
        else:
            while len(l)<7:
                l=[0]+l
            return l
    def producto_interno(l,m,q):
        return sum([l[i]*m[i] for i in range(0,q)])
    l=[2,9,8,7,6,3,4]
    def digito_verificador(n):
        m=completa_lista(n)
        p=producto_interno(l,m,7)
        return (10-p%10)%10
    def ci_igual_terminacion(n):
        m=completa_lista(n)
        s=producto_interno(l,m,4)
        return [(x,y,z,t,m[4],m[5],m[6]) for x in range(0,10) for y in range(0,10) for
    z in range(0,10) for t in range(0,10) if (producto_interno(l,[x,y,z,t],4))%10==s
    %10]
    while ci not in range(0,10000000):
        print "Debe ingresar un número de Cédula de Identidad válido."; print
        ci=input("Número de Cédula de Identidad: ")
        print
    tiempo_inicial=time()
    y=digito_verificador(ci)
    print "El dígito verificador de su número de Cédula de Identidad es", y; print
    t=ci_igual_terminacion(ci)
    z=completa_lista(ci)
    print "Además, existen", len(t), "números de Cédula de Identidad (incluyendo la
    suya) con la terminación", z[4], z[5], z[6], "-", y, "y son:"; print
    for i in range(0,len(t)):
        r=t[i]
        print r[0],".",r[1],r[2],r[3],".",r[4],r[5],r[6],"-",y
    tiempo_final=time()
    tiempo_total=tiempo_final-tiempo_inicial
    print; print "El tiempo de ejecución fue de", tiempo_total, "segundos."
    print; print "Presione la tecla s para salir o cualquier otra tecla para continuar.
     Luego presione Enter."
    print
    fin=raw_input("¿Desea salir de este programa? ")
    print
```

Figura 1. Código en lenguaje Python

Por último, las siguientes imágenes muestran los resultados que acabamos de indicar, luego de ejecutado el programa:

6. Conclusiones

En el desarrollo anterior se ha probado que, en teoría, para todo número de C.I. de la forma $a\,.\,b\,c\,d\,.\,e\,f\,g\,-\,X$, existen exactamente 1000 números de C.I. (incluido el número de C.I. dado) con idéntica terminación ($e\,f\,g\,-\,X$), con a, b, c, d, e, f, g y X naturales menores que 10.

La expresión *en teoría* hace referencia a que, en realidad, la numeración de la C.I. es asignada por la *Dirección Nacional de Identificación Civil* del Uruguay y, teniendo en cuenta que la población

```
duberlygonzalezmolinari — cedula_de_identidad.py — 110×36
Last login: Sat Mar 10 00:11:04 on ttys000
air-de-duberly:~ duberlygonzalezmolinari$ python /Users/duberlygonzalezmolinari/Desktop/cedula_de_identidad.py


Ingrese su número de Cédula de Identidad sin puntos ni guión ni dígito verificador. Luego presione Enter.

Ejemplo: Si su número de Cédula de Identidad es 1.234.567-8, debe ingresar 1234567

Número de Cédula de Identidad: 4378273

El dígito verificador de su número de Cédula de Identidad es 8

Además, existen 1000 números de Cédula de Identidad (incluyendo la suya) con la terminación 2 7 3 - 8 y son:

0 . 0 0 1 . 2 7 3 - 8
0 . 0 1 7 . 2 7 3 - 8
0 . 0 2 3 . 2 7 3 - 8
0 . 0 3 9 . 2 7 3 - 8
0 . 0 4 5 . 2 7 3 - 8
0 . 0 5 1 . 2 7 3 - 8
0 . 0 6 7 . 2 7 3 - 8
0 . 0 7 3 . 2 7 3 - 8
0 . 0 8 9 . 2 7 3 - 8
0 . 0 9 5 . 2 7 3 - 8
0 . 1 0 4 . 2 7 3 - 8
0 . 1 1 0 . 2 7 3 - 8
0 . 1 2 6 . 2 7 3 - 8
0 . 1 3 2 . 2 7 3 - 8
0 . 1 4 8 . 2 7 3 - 8
0 . 1 5 4 . 2 7 3 - 8
0 . 1 6 0 . 2 7 3 - 8
0 . 1 7 6 . 2 7 3 - 8
0 . 1 8 2 . 2 7 3 - 8
0 . 1 9 8 . 2 7 3 - 8
0 . 2 0 7 . 2 7 3 - 8
```

Figura 2. Inicio de la ejecución del programa.

```
duberlygonzalezmolinari — cedula_de_identidad.py — 110×36
9 . 7 0 8 . 2 7 3 - 8
9 . 7 1 4 . 2 7 3 - 8
9 . 7 2 0 . 2 7 3 - 8
9 . 7 3 6 . 2 7 3 - 8
9 . 7 4 2 . 2 7 3 - 8
9 . 7 5 8 . 2 7 3 - 8
9 . 7 6 4 . 2 7 3 - 8
9 . 7 7 0 . 2 7 3 - 8
9 . 7 8 6 . 2 7 3 - 8
9 . 7 9 2 . 2 7 3 - 8
9 . 8 0 1 . 2 7 3 - 8
9 . 8 1 7 . 2 7 3 - 8
9 . 8 2 3 . 2 7 3 - 8
9 . 8 3 9 . 2 7 3 - 8
9 . 8 4 5 . 2 7 3 - 8
9 . 8 5 1 . 2 7 3 - 8
9 . 8 6 7 . 2 7 3 - 8
9 . 8 7 3 . 2 7 3 - 8
9 . 8 8 9 . 2 7 3 - 8
9 . 8 9 5 . 2 7 3 - 8
9 . 9 0 4 . 2 7 3 - 8
9 . 9 1 0 . 2 7 3 - 8
9 . 9 2 6 . 2 7 3 - 8
9 . 9 3 2 . 2 7 3 - 8
9 . 9 4 8 . 2 7 3 - 8
9 . 9 5 4 . 2 7 3 - 8
9 . 9 6 0 . 2 7 3 - 8
9 . 9 7 6 . 2 7 3 - 8
9 . 9 8 2 . 2 7 3 - 8
9 . 9 9 8 . 2 7 3 - 8

El tiempo de ejecución fue de 0.02800989151 segundos.

Presione la tecla s para salir o cualquier otra tecla para continuar. Luego presione Enter.

¿Desea salir de este programa?
```

Figura 3. Fin de la ejecución del programa.

total de dicho país era de 3.286.314 habitantes en el año 2011[2], y que la C.I. es obligatoria a partir de los 45 días de nacimiento, no es real que existan exactamente diez millones de cédulas de identidad vigentes.

Por tanto, de manera ideal, suponiendo que yo participo con la terminación de mi C.I. ($273-8$) en un sorteo a través de internet de las características ya comentadas, cabe plantearse la siguiente pregunta: ¿Cuál es la probabilidad de que otra persona con idéntica terminación de C.I. participe en el mismo sorteo?

Por una parte, tenemos que existe un total de 999 *casos favorables* (todos los números de C.I. con la terminación $273-8$, excepto la mía), y un total de 9.999.999 *casos posibles* (todos los números de C.I. posibles, excepto la mía).

De esta manera, la probabilidad de ocurrencia del suceso $A =$ "Participa de un sorteo de las características ya mencionadas una persona con idéntica terminación de C.I. que la mía, habiendo yo participado" es:

$$P(A) = \frac{999}{9.999.999} \approx 0,01\,\%$$

es decir, un número relativamente pequeño.

En resumen, esta forma de identificarse en la participación de los sorteos por internet u otro medio es, por tanto, bastante segura aunque no 100 % confiable.

Referencias

[1] FERNÁNDEZ, W., *Matemática II de Bachillerato 2º Año Diversificación Científica*, 3ª Edición. Ediciones del Palacio, Montevideo, Uruguay, 2015.

[2] OSÍN, L., *Introducción al Análisis Matemático*, 1ª Edición. Editorial Kapelusz, Buenos Aires, Argentina, 1966.

[3] RIVERO, F., *Introducción a la teoría de números*, Capítulo II: Congruencias. 1ª Edición. Editor SABER ULA, Mérida, Venezuela, 2006.

Sobre el autor:
Nombre: Duberly González Molinari
Correo electrónico: duberly@gmail.com
Institución: Profesor de Matemática en el Consejo de Educación Secundaria de la República Oriental del Uruguay.

[2]Véase: `http://www.ine.gub.uy/documents/10181/35289/analisispais.pdf/cc0282ef-2011-4ed8-a3ff-32372d31e690`